



UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/511,105	10/14/2004	Jukka Tuomi	60091.00338	6584
32294	7590	11/28/2007		
SQUIRE, SANDERS & DEMPSEY L.L.P. 14TH FLOOR 8000 TOWERS CRESCENT TYSONS CORNER, VA 22182			EXAMINER AJIBADE AKONAI, OLUMIDE	
			ART UNIT 2617	PAPER NUMBER
			MAIL DATE 11/28/2007	DELIVERY MODE PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Office Action Summary

Application No.

10/511,105

Applicant(s)

TUOMI ET AL.

Examiner

Olumide T. Ajibade-Akonai

Art Unit

2617

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

- 1) ☒ Responsive to communication(s) filed on 13 September 2007.
- 2a) ☐ This action is FINAL. 2b) ☒ This action is non-final.
- 3) ☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

- 4) ☒ Claim(s) 2-12,14,21-23,25-38 and 45-47 is/are pending in the application.
- 4a) Of the above claim(s) _____ is/are withdrawn from consideration.
- 5) ☒ Claim(s) 2-12,14,21-23,25-38 and 45-47 is/are allowed.
- 6) ☒ Claim(s) 13 is/are rejected.
- 7) ☐ Claim(s) _____ is/are objected to.
- 8) ☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

- 9) ☐ The specification is objected to by the Examiner.
- 10) ☐ The drawing(s) filed on _____ is/are: a) ☐ accepted or b) ☐ objected to by the Examiner.
Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).
Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).
- 11) ☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

- 12) ☒ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).
- a) ☒ All b) ☐ Some * c) ☐ None of:
1. ☒ Certified copies of the priority documents have been received.
 2. ☐ Certified copies of the priority documents have been received in Application No. _____.
 3. ☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).
- * See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

- | | |
|--|---|
| 1) <input checked="" type="checkbox"/> Notice of References Cited (PTO-892) | 4) <input type="checkbox"/> Interview Summary (PTO-413)
Paper No(s)/Mail Date. _____ |
| 2) <input type="checkbox"/> Notice of Draftsperson's Patent Drawing Review (PTO-948) | 5) <input type="checkbox"/> Notice of Informal Patent Application |
| 3) <input type="checkbox"/> Information Disclosure Statement(s) (PTO/SB/08)
Paper No(s)/Mail Date _____ | 6) <input type="checkbox"/> Other: _____ |

DETAILED ACTION

Claim Rejections - 35 USC § 103

1. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

(a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negated by the manner in which the invention was made.

The factual inquiries set forth in *Graham v. John Deere Co.*, 383 U.S. 1, 148 USPQ 459 (1966), that are applied for establishing a background for determining obviousness under 35 U.S.C. 103(a) are summarized as follows:

1. Determining the scope and contents of the prior art.
2. Ascertaining the differences between the prior art and the claims at issue.
3. Resolving the level of ordinary skill in the pertinent art.
4. Considering objective evidence present in the application indicating obviousness or nonobviousness.

This application currently names joint inventors. In considering patentability of the claims under 35 U.S.C. 103(a), the examiner presumes that the subject matter of the various claims was commonly owned at the time any inventions covered therein were made absent any evidence to the contrary. Applicant is advised of the obligation under 37 CFR 1.56 to point out the inventor and invention dates of each claim that was not commonly owned at the time a later invention was made in order for the examiner to consider the applicability of 35 U.S.C. 103(c) and potential 35 U.S.C. 102(e), (f) or (g) prior art under 35 U.S.C. 103(a).

2. Claim is 13, 22, 23, 37, 46, and 47 are rejected under 35 U.S.C. 103(a) as being unpatentable over **McCann et al EP 1191763 (hereinafter McCann)** in view of **Shirai 5,828,956**.

Regarding **claim 13**, McCann discloses a method for authenticating a user of a data transfer device, comprising: setting up a data transfer connection from the data transfer device (portable device, see fig. 1, col. 3, [0013]) to a service access point (communication between the portable device and the SSG using a secure communication protocol, see col. 3, [0015]); inputting identification data (WLAN identity, see fig. 1, col. 3, [0014]) of a subscriber of a mobile communications system (mobile user with handset 10, see fig. 1, col. 3, [0017]) to the service access point (service selection gateway SSG 5, see fig. 1, col. 3, [0015]); checking from the mobile communications system whether the mobile subscriber identification data contains an access right to the service access point (see fig. 1, col. 3, [0016]-[0017]); and, if a valid access right exists, generating a password (PIN, see fig. 1, col. 3, [0017]), transmitting the password to a subscriber terminal corresponding to the mobile subscriber identification data (see fig. 1, col. 3, [0017]), and logging in to the service access point from the data transfer device using the password transmitted to the subscriber terminal (mobile user utilizes the sent PIN for validation of WLAN account, see fig. 1, col. 3, [0017]).

McCann fails to disclose transmitting a second password from the service access point to the data transfer device over a data transfer connection, the second password being also used in connection with login.

In a similar field of endeavor, Shirai teaches a method of transmitting a second password (transmitting two passwords to a mobile phone user, see col. 13, lines 61-17) from the service access point (service center, see col. 13, lines 61-67) to the data transfer device (mobile phone, see fig. 2, col. 13, lines 53-58) over a data transfer connection, the second password being also used in connection with login (providing two passwords to a user of a mobile phone so that the user can have access to the network, see col. 13, lines 59-67, and col. 14, lines 1-18)).

It would therefore have been obvious to one of ordinary skill in the art, at the time the invention was made, to combine the teaching Shirai, by providing two passwords to mobile device for benefit of providing a mobile device with proper access to a network operator.

Allowable Subject Matter

3. Claims 2-12, 14, 21-23, 25-38, and 45-47 are allowed.

The following is an examiner's statement of reasons for allowance: Regarding **claim 14, McCann et al EP 1191763** discloses a method for authenticating a user of a data transfer device, comprising: setting up a data transfer connection from the data transfer device to a service access point; inputting identification data of a subscriber of a mobile communications system to the service access point; checking from the mobile communications system whether the mobile subscriber identification data contains an access right to the service access point; and, if a valid access right exists, generating a password, transmitting the password to a subscriber terminal corresponding to the

mobile subscriber identification data, and logging in to the service access point from the data transfer device using the password transmitted to the subscriber terminal. The instant invention discloses transmitting a confirmation identifier from the service access point to the data transfer device over a data transfer connection and transmitting the same confirmation identifier to the subscriber terminal together with the password, the password being only used if the received confirmation identifiers are the same. The above novel features in combination with all the other recited limitations is neither taught, suggested, nor made obvious by McCann or any other prior art of record. Claims 2-12 and 21 are allowable based on their being dependent on claim 14.

Regarding **claim 22, McCann et al EP 1191763** discloses a method for authenticating a user of a data transfer device, comprising: setting up a data transfer connection from the data transfer device to a service access point; inputting identification data of a subscriber of a mobile communications system to the service access point; checking from the mobile communications system whether the mobile subscriber identification data contains an access right to the service access point; and, if a valid access right exists, generating a password, transmitting the password to a subscriber terminal corresponding to the mobile subscriber identification data, and logging in to the service access point from the data transfer device using the password transmitted to the subscriber terminal. The instant invention discloses transmitting a user identification to the subscriber terminal corresponding to the mobile subscriber identification information data and using the transmitted user identification in connection with login. The above novel features are in combination with all the other recited

limitations is neither taught, suggested, nor made obvious by McCann or any other prior art of record.

Regarding **claim 23, McCann et al EP 1191763** discloses a method for authenticating a user of a data transfer device, comprising: setting up a data transfer connection from the data transfer device to a service access point; inputting identification data of a subscriber of a mobile communications system to the service access point; checking from the mobile communications system whether the mobile subscriber identification data contains an access right to the service access point; and, if a valid access right exists, generating a password, transmitting the password to a subscriber terminal corresponding to the mobile subscriber identification data, and logging in to the service access point from the data transfer device using the password transmitted to the subscriber terminal. The instant invention discloses transmitting a user identification to the data transfer device over a data transfer connection and using the transmitted user identification in connection with login. The above novel features are in combination with all the other recited limitations is neither taught, suggested, nor made obvious by McCann or any other prior art of record.

Regarding **claim 37, McCann et al EP 1191763** discloses a system configured to authenticate a user of a data transfer device, comprising: a data transfer device; a service access point that can be linked to the data transfer device over a first data transfer connection; and an authentication server linked to the service access point over a second data transfer connection, wherein the service access point is configured to receive over the first data transmission connection identification data of a subscriber of

a mobile communications system inputted from the data transfer device and to transmit the mobile subscriber identification data to the authentication server over the second data transfer connection, the authentication server is configured to check from the mobile communications system over a third data transfer connection whether the mobile subscriber identification data contains an access right to the service access point and, if a valid access right exists, to generate a password and transmit the password to a subscriber terminal corresponding to the identification data of the subscriber of the mobile communications system, the data transfer device is configured to use the password transmitted to the subscriber terminal in connection with login to the service access point. The instant invention discloses the authentication server is configured to transmit a second password from the service access point to the data transfer device over the first data transfer connection and the data transfer device is configured to also use the second password in connection with login. The above novel features are in combination with all the other recited limitations is neither taught, suggested, nor made obvious by McCann or any other prior art of record.

Regarding **claim 38**, **McCann et al EP 1191763** discloses a system configured to authenticate a user of a data transfer device, comprising: a data transfer device; a service access point that can be linked to the data transfer device over a first data transfer connection; and an authentication server linked to the service access point over a second data transfer connection, wherein the service access point is configured to receive over the first data transmission connection identification data of a subscriber of a mobile communications system inputted from the data transfer device and to transmit

the mobile subscriber identification data to the authentication server over the second data transfer connection, the authentication server is configured to check from the mobile communications system over a third data transfer connection whether the mobile subscriber identification data contains an access right to the service access point and, if a valid access right exists, to generate a password and transmit the password to a subscriber terminal corresponding to the identification data of the subscriber of the mobile communications system, the data transfer device is configured to use the password transmitted to the subscriber terminal in connection with login to the service access point. The instant invention discloses the authentication server is configured to transmit a confirmation identifier via the service access point to the data transfer device over the first data transfer connection and to transmit the same confirmation identifier to the subscriber terminal together with the password. The above novel features are in combination with all the other recited limitations is neither taught, suggested, nor made obvious by McCann or any other prior art of record. Claims 25-36, and 45 are allowable based on their being dependent on claim 38.

Regarding **claim 46**, **McCann et al EP 1191763** discloses a system configured to authenticate a user of a data transfer device, comprising: a data transfer device; a service access point that can be linked to the data transfer device over a first data transfer connection; and an authentication server linked to the service access point over a second data transfer connection, wherein the service access point is configured to receive over the first data transmission connection identification data of a subscriber of a mobile communications system inputted from the data transfer device and to transmit

the mobile subscriber identification data to the authentication server over the second data transfer connection, the authentication server is configured to check from the mobile communications system over a third data transfer connection whether the mobile subscriber identification data contains an access right to the service access point and, if a valid access right exists, to generate a password and transmit the password to a subscriber terminal corresponding to the identification data of the subscriber of the mobile communications system, the data transfer device is configured to use the password transmitted to the subscriber terminal in connection with login to the service access point. The instant invention discloses the authentication server is configured to transmit a user identification to the subscriber terminal corresponding to the mobile subscriber identification information data and using the transmitted user identification in connection with login. The above novel features are in combination with all the other recited limitations is neither taught, suggested, nor made obvious by McCann or any other prior art of record.

Regarding **claim 47, McCann et al EP 1191763** discloses a system configured to authenticate a user of a data transfer device, comprising: a data transfer device; a service access point that can be linked to the data transfer device over a first data transfer connection; and an authentication server linked to the service access point over a second data transfer connection, wherein the service access point is configured to receive over the first data transmission connection identification data of a subscriber of a mobile communications system inputted from the data transfer device and to transmit the mobile subscriber identification data to the authentication server over the second

data transfer connection, the authentication server is configured to check from the mobile communications system over a third data transfer connection whether the mobile subscriber identification data contains an access right to the service access point and, if a valid access right exists, to generate a password and transmit the password to a subscriber terminal corresponding to the identification data of the subscriber of the mobile communications system, the data transfer device is configured to use the password transmitted to the subscriber terminal in connection with login to the service access point. The instant invention discloses the authentication server is configured to transmit the user identification via the service access point to the data transfer device over the first data transfer connection and the data transfer device is configured to use the user identification transmitted to the data transfer device in connection with login to the service access point. The above novel features are in combination with all the other recited limitations is neither taught, suggested, nor made obvious by McCann or any other prior art of record.

Any comments considered necessary by applicant must be submitted no later than the payment of the issue fee and, to avoid processing delays, should preferably accompany the issue fee. Such submissions should be clearly labeled "Comments on Statement of Reasons for Allowance."

Response to Arguments

4. Applicant's arguments see pages 29-31 of the remarks, filed 13 September 2007, with respect to claims 13, 22, 23, 37, 46, and 47 have been fully considered and are

persuasive. The 35 U.S.C § 103(a) rejection of claims 13, 22, 23, 37, 46, and 47 has been withdrawn.

Applicant's arguments, see pages 29-31 of the remarks, filed 13 September 2007, with respect to the rejection(s) of claim(s) 13 under 35 U.S.C § 103(a) have been fully considered and are persuasive. Therefore, the rejection has been withdrawn. However, upon further consideration, a new ground(s) of rejection is made in view of McCann et al EP 1191763 and Shirai 5,828,956.

Applicant's arguments, see pages 27-28 of the remarks filed 13 September 2007 have been fully considered but they are not persuasive. Regarding claim 13, the applicant's representative asserts that McCann fails to teach or suggest, "if a valid access right exists, generating a password, transmitting the password to a subscriber terminal corresponding to the mobile subscriber identification data, and logging in to the service access point from the data transfer device using the password transmitted to the subscriber terminal". The examiner respectfully disagrees. The PIN in McCann is transmitted through the SMSC 9 to the mobile user on the handset 10. The PIN is used the mobile to validate the portable handset's entry to a cellular account (see figs. 1 and 2, col. 3, [0013], [0017], col. 4, [0025]-[0026]). This broadly reads on the claimed invention of "generating a password, transmitting the password to a subscriber terminal corresponding to the mobile subscriber identification data, and logging in to the service access point from the data transfer device using the password transmitted to the subscriber terminal", since as the password is used by the subscriber terminal to

validate or login to a service access point. McCann therefore meets the claimed limitation as disclosed.

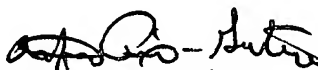
Conclusion

5. Any inquiry concerning this communication or earlier communications from the examiner should be directed to Olumide T. Ajibade-Akonai whose telephone number is 571-272-6496. The examiner can normally be reached on M-F, 8.30p-5p.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Rafael Perez-Gutierrez can be reached on 571-272-7915. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see <http://pair-direct.uspto.gov>. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

OA
OA


Rafael Perez-Gutierrez
Supervisory Patent Examiner
Technology Center 2600
Art Unit 2617

11/26/12